Michigan Telecommunications and Technology Law Review

Volume 23 | Issue 2

2017

Jailbreak!: What Happens When Autonomous Vehicle Owners Hack Into Their Own Cars

Michael Sinanian
University of Michigan Law School

NOTE

JAILBREAK!: WHAT HAPPENS WHEN AUTONOMOUS VEHICLE OWNERS HACK INTO THEIR OWN CARS

*Michael Sinanian**

Cite as: Michael Sinanian, Note,
Jailbreak!: What Happens When Autonomous Vehicle Owners Hack Into Their Own Cars,
23 MICH. TELECOM. & TECH. L. REV. 357 (2017).
This manuscript may be accessed online at repository.law.umich.edu.

ABSTRACT

Autonomous and connected vehicles (ACVs) are a transformational force for humanity. It is highly likely that some owners of ACVs will circumvent their vehicle software to expose unauthorized functionality, known as "jailbreaking". This would trigger copyright liability, the extent of which would be dependent upon the copyright system's various rulemaking processes and common law interpretations. This note explores the world of software "jailbreaking", with its roots in smartphone unlocking, and extrapolates that to ACVs. Some compelling (and at times dangerous) scenarios are contemplated, and recommendations are made for consumers, technologists, manufacturers, and policy makers.

TABLE OF CONTENTS

---

* I would like to thank a few authors who have penned major foundational works in this area. The source from which I draw most from is *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, written by a team of professors, Professors Crane, Logue, and Pilz, hailing from my own institution, the University of Michigan Law School. *See infra* note 111. I also derived a fair bit from Dorothy Glancy's *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem* (*see infra* at note 37), in addition to Jeffrey Gurney's *Crashing into the Unknown: An Examination of Crash-Optimization Algorithms Through the Two Lanes of Ethics and Law*. *See infra* note 42. I also owe thanks to Anderson, et al.'s report *Autonomous Vehicle Technology: A Guide for Policymakers* published through Rand. *See infra* note 2.

I. Introduction

This paper aims to explore the legal repercussions of jailbreaking Autonomous and Connected Vehicles ("ACVs"), as applied to those who develop, distribute, install, and use such software. Jailbreaking is the act of lifting manufacturer-imposed restrictions on software operating systems, unlocking a host of latent, unauthorized capabilities.[1] ACV jailbreaking is an important concern because ACVs will transform automotive transportation as we know it. ACVs are one of the major technological leaps of our lifetime, ushering in an era where crashes rarely ever result in fatalities,[2] cities are transformed by new land use patterns,[3] and consumers are spared the burdensome cost of motor vehicle ownership,[4] among countless other benefits. They will also dramatically reshape the economy.[5]

1. Jailbreaks are fundamentally different from cyberattacks. Technologically speaking, the acts are similar, but from both a practical and legal standpoint, they are entirely different. The distinction is best captured by intention – cyberattacks are a malicious, unwanted event that could occur to ACVs, while jailbreaking is a user-initiated event upon a vehicle users already own to achieve their desired aims. Jailbreakers *willingly* install, use, and take advantage of the circumvention's capabilities.

2. *See* James M. Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, at xiv Rand (2016), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf.

3. *Id.* at xvi (explaining that "[ACVs] may lead to increased density as a result of the decreased need for proximate parking . . . [since] approximately 31 percent of space in the central business districts of 41 major cities was devoted to parking" (citing Shoup, 2005)).

4. *Id.* at 19.

5. ACVs are expected to displace 5 million jobs in the transportation industry, which accounts for 3% of the workforce. "Auto dealerships, car washes, gas stations, and parking lots might shut down completely," eliminating even more collateral jobs. Steven Greenhouse, *Autonomous vehicles could cost America 5 million jobs. What should we do about it?,* L.A. Times

The technological development and deployment of ACVs will be a mixed process – there is no one path to ACV adoption. One deployment scenario is for transportation network companies ("TNCs"), such as Uber and Lyft, which provide mobile applications to connect passengers to drivers, to convert their fleet of human-driven vehicles into ACVs.[6] This model would not give rise to jailbreaking, since TNCs would be in complete control of their vehicles. However, there will be some period of time in which the current model of individually owned vehicles will continue, only that such vehicles will become ACVs. This is a necessary condition for the jailbreaking contemplated in this paper, since only individual ACV owners would jailbreak their own vehicles.

There are compelling reasons for ACV owners to jailbreak their vehicles. Some of these are relatively innocuous and coincide with societal norms of product ownership, while others present the potential for serious harms and raise serious moral questions, such as programming a vehicle to prioritize a passenger over a pedestrian in a "no-win" collision scenario. Harms include economic loss, property damage, personal injury, and death. The risk of these harms is unlike the circumvention of other types of electronic machinery, such as smartphone jailbreaking.

Circumvention of electronics is governed by the Digital Millennium Copyright Act ("DMCA"), and ACV jailbreaks would be subject to this law. However, it is not equipped to deal with circumventions that could lead to the serious harms and moral dilemmas just described. It is therefore necessary to propose new legislation or regulation to handle this unique circumstance, outside the ambit of the copyright system. Technologists and policy makers both should play an active part in shaping such laws.

Some terminology in this report merits clarification. The term "ACV companies" refers to ACV manufacturers, component/parts suppliers, software providers, transportation network companies, and other businesses in the ACV ecosystem collectively. Manufacturers are referred to as original

---

(Sept. 22, 2016), http://www.latimes.com/opinion/op-ed/la-oe-greenhouse-driverless-job-loss-20160922-snap-story.html.

6. These types of companies have rapidly become more involved in ACV development and deployment, since integrating autonomous capabilities into their fleet would eliminate the high cost of employing human drivers. Uber, in partnership with Volvo, and with the help of a team of roboticists lured away from Carnegie Mellon University, is deploying autonomous custom Volvo XC90 vehicles in Pittsburgh, supervised by humans in the "driver's" seat. *See* Max Chafkin, *First Self-Driving Fleet Arrives in Pittsburgh This Month*, BLOOMBERG (Aug. 18, 2016), https://www.bloomberg.com/news/features/2016-08-18/uber-s-first-self-driving-fleet-arrives-in-pittsburgh-this-month-is06r7on; *See also* John Zimmer, *The Third Transportation Revolution: Lyft's Vision for the Next Ten Years and Beyond*, MEDIUM (Sept. 18, 2016), https://medium.com/@johnzimmer/the-third-transportation-revolution-27860f05fa91; *See also* Jake Maxwell Watts, *World's First Self-Driving Taxis Hit the Road in Singapore*, WALL ST. J. (Aug. 25, 2016, 6:51AM), https://www.wsj.com/articles/worlds-first-self-driving-taxis-hit-the-road-in-singapore-1472102747.

equipment manufacturers ("OEMs"), when it is important to distinguish them from other ACV companies.

II. BACKGROUND

A. *The Dawn of ACVs*

Since Google unveiled its autonomous vehicle project in 2010, there has been steady progress across both the automotive and software industries to develop this technology, with support from research universities as well as state and federal governments.[7] The utility of ACVs is without question: their widespread deployment would sharply curtail traffic fatalities, reclaim much-needed space in urban environments, and provide a host of other benefits.[8]

The World Health Organization estimates that 1.25 million people die from auto-related accidents each year, with half of these deaths being pedestrians, bicyclists, and motorcyclists.[9] Vehicles are the leading cause of death for people between 15 to 29 years old.[10] On a miles-driven basis, ACVs are potentially far safer than human-driven motor vehicles, and are not prone to human fallibilities like driving while intoxicated, drowsy, or distracted.[11] Global ACV adoption would thus potentially improve these grim statistics.[12] It is estimated that by 2035, 75 percent of vehicles will possess some degree of autonomous capability.[13]

Today, motor vehicles are mostly owned by the same people who operate them: consumers. For some period of time during the progression of ACV technology, consumers will continue to be the predominant owners and operators of motor vehicles, but at some point, different deployment patterns will emerge, including that of TNCs, discussed in the introduction.

ACV manufacturers will gradually increase their vehicles' autonomous capabilities, some of which are already found in today's vehicles.[14] Eventually, these vehicles will become fully autonomous. Tesla Motors' Model S is

---

7. John Markoff, *Google Cars Drive Themselves, in Traffic*, N.Y. TIMES (Oct. 9, 2010), http://www.nytimes.com/2010/10/10/science/10google.html.

8. *See* Anderson et al., *supra* note 2.

9. *See* WHO, *Global Status Report on Road Safety 2015* at 2 (2015), http://www.who.int/violence_injury_prevention/road_safety_status/2015/GSRRS2015_Summary_EN_final.pdf.

10. *See id.*

11. *See* Anderson et al., *supra* note 2, at 12.

12. *See* Matt McFarland, *How Self-Driving Cars Would Benefit Americans More Than World Peace,* WASH. POST. (Feb. 10, 2015), http://www.washingtonpost.com/blogs/innovations/wp/2015/02/10/how- self-driving-cars-would-benefit-americans-more-than-world-peace/.

13. *See* Richard Martin, *Three-Quarters of Vehicles Sold in 2035 Are Expected to Have Autonomous Capability*, NAVIGANT CONSULTING (Nov. 6, 2014), https://www.navigantresearch.com/newsroom/three-quarters-of-vehicles-sold-in-2035-are-expected-to-have-autonomous-capability.

14. *Id.* at 5.

an example of this development roadmap.[15] It is equipped with hardware that evolves through the periodic introduction of software updates.[16] Such a software model necessitates a whole-car operating system that invites circumvention, as opposed to having to circumvent each automotive component piecemeal, as is required by today's automobiles. In fact, such operating systems will be a key component in the ACV supply chain, with both automotive and technology companies vying to dominate the market.[17]

B. *Reasons to Jailbreak*

A jailbreak is a version of the operating system with the OEM's default restrictions lifted, allowing for a number of factory-unauthorized functions. The term stems from the idea that a device is broken out of its "jail".[18] There are many compelling reasons for ACV owners to jailbreak their vehicles. These include overriding traffic safety programming, enabling high performance driving, circumscribing statutory controls on driving times and locations, disabling location tracking for privacy, hiding from law enforcement, and prioritizing vehicle occupants over potential victims in a crash scenario.

1. Smartphone Jailbreaking

Since the debut of the Apple iPhone in 2007, people have found ways to lift the software restrictions imposed by iOS, the device's operating system, and extend the functionality of their smartphones.[19] This activity did not have the protection of the copyright system until 2010.[20]

In the smartphone context, jailbreaking has been used to unlock all sorts of functionality.[21] On the iPhone, jailbreaking allows the installation of unapproved apps. It also allows users to apply custom visual themes. In the

15. *See* The Tesla Motors Team, *Your Autopilot has Arrived*, THE TESLA BLOG (Oct. 14, 2015), https://www.teslamotors.com/blog/your-autopilot-has-arrived/; *See also* Tim Higgins, *Tesla Expects to Demonstrate Self-Driven Cross-Country Trip Next Year,* WALL ST. J. (Oct. 19, 2016), http://www.wsj.com/articles/tesla-expects-to-demonstrate-self-driven-cross-country-trip-next-year-1476925700.

16. The Tesla Motors Team, *supra* note 16.

17. ECONOMIST, *Who's self-driving your car?* (Sept. 24, 2016), http://www.economist.com/news/business/21707600-battle-driverless-cars-revs-up-whos-self-driving-your-car ("All parties recognize that the biggest profits from autonomy will come from producing an 'operating system'—something that integrates the software and algorithms that process and interpret information from sensors and maps and the mechanical parts of the car. Tech firms probably have the edge here.").

18. *See* Mike Keller, *Geek 101: What Is Jailbreaking?*, PCWORLD (Feb. 13, 2012), http://www.pcworld.com/article/249091/geek_101_what_is_jailbreaking_.html.

19. In 2010, about 10 percent of all iPhone users had jailbroken their devices. *See* Deb Shindler, *Pros and Cons of Jailbreaking or Rooting Your Smartphone*, TECHREPUBLIC (Aug. 20, 2010, 1:00 PM), http://www.techrepublic.com/blog/smartphones/pros-and-cons-of-jailbreaking-or-rooting-your-smartphone/.

20. *See* Jenna Wortham, *In Ruling on iPhones, Apple Loses a Bit of Its Grip,* N.Y. TIMES (July 26, 2010), http://www.nytimes.com/2010/07/27/technology/27iphone.html.

21. *See* Shindler, *supra* note 19.

early days, it allowed users to sort apps into folders, years before such functionality was available. Perhaps the most enticing use of a jailbroken phone is to unlock it from its carrier, allowing the device to be used on other carriers without having to pay for a separate carrier-specific device.[22] On the Android platform, "rooting" (the Android equivalent of jailbreaking) allows for drastic boosts to performance and battery life.[23] Since the vanilla operating system must cater to hundreds of millions of users, conservative defaults are used for these parameters, but jailbreaking/rooting allows for user-specific customization.

OEMs have been reluctant to tolerate this activity. Apple in particular is engaged in a decade-long arms race with the iOS jailbreaking community, with one side finding a new way to gain access and the other patching it, ad infinitum[24] Apple itself has *not* legally threatened this enthusiast community. It has even on multiple occasions thanked it for finding software security vulnerabilities ("bugs") in iOS, with the gratitude mentioned in the release notes of a software update.[25] It has also gone so far as to hire a member of the jailbreak community.[26]

OEMs could similarly "collaborate" with the jailbreaking community, benefiting from their detection of bugs which could otherwise be used by malicious actors in a cyberattack. As in smartphone jailbreaking, such activ-

22. This function has since been legalized by an act of Congress, the Unlocking Consumer Choice and Wireless Competition Act of 2014, which overrides the Library of Congress's rules on the matter. Unlocking Consumer Choice and Wireless Competition Act, Pub.L. 113–144, 128 Stat. 1751 (2014).

23. Both "rooting" and "jailbreaking" can be used interchangeably, and in the context of this paper, jailbreaking will be the term used. "Unlocking" a smartphone so that it works across multiple cellular carriers instead of being locked into just one is recognized as a variant of jailbreaking, and all instances of jailbreaking in this paper will be inclusive of unlocking.

24. It should be noted that the incentive to jailbreak smartphones has decreased considerably over time, as manufacturers have slowly added the functionality that users were originally installing jailbroken OSs for. *See* Kim-Mai Cutler, *Umeng, The Flurry of China, Says iOS Jailbreaking Is On The Decline,* TECHCRUNCH (Nov. 14, 2012), https://techcrunch.com/2012/11/14/umeng-jailbreaking/.

25. *See* Filip Truta, *Apple Thanks PanguTeam for Exposing iOS Flaw, Kills Their Jailbreak,* SOFTPEDIA (Nov. 18, 2014 14:41 GMT), http://news.softpedia.com/news/Apple-Thanks-PanguTeam-for-Exposing-iOS-Flaw-Kills-their-Jailbreak-465274.shtml; *See also* Luke Dormehl, *Apple Thanks Jailbreakers for Tightening Up iOS 7.1 Security*, CULT OF MAC (Mar. 11, 2014, 3:03 AM), http://www.cultofmac.com/269479/apple-thanks-jailbreakers-tightening-ios-7-1-security/; *See also* Matthew Panzarino, *Apple credits evad3rs jailbreak team with 4 of 6 software bugs fixed in iOS 6.1.3,* THE NEXT WEB (Mar. 19, 2013), http://thenextweb.com/apple/2013/03/19/apple-credits-evad3rs-jailbreak-team-with-4-of-6-software-bugs-fixed-in-ios-6-1-3/.

26. *See* Jeff Benjamin, *iOS jailbreak hacker Winocm joining Apple later this year*, IDOWNLOADBLOG (Feb. 21, 2014), http://www.idownloadblog.com/2014/02/21/ios-jailbreak-hacker-winocm-joining-apple-later-this-year/.

ity for ACVs would still be prohibited by contract, but companies may merely turn a blind eye.[27]

2. ACV-specific Incentives

Like for smartphones, jailbreaking ACVs may confer a number of advantages to end-users.[28] The incentives may be strong enough to compel end-users to violate the law. The governing legal framework of jailbreaking, copyright law, is likely insufficient to deter this activity.

For example, ACVs will likely be programmed to comply with all traffic laws and regulations, but an end user may attempt to override that programming, ostensibly to get somewhere faster. The incentive to do so may be strong enough despite the potential for criminal liability.[29]

Extending the idea of overriding traffic laws, an ACV jailbreak may even allow for a "performance racing mode", whereby an ACV is programmed to drive as if it were in NASCAR or Le Mans. Most drivers do not possess the ability to drive at a professional level, but such a feature could offer this unique experience. This is a novel scenario we are yet to witness on public roadways.[30]

Another use would be to route around legislatively proscribed limitations on where and when ACVs could be used. It is possible for governments to pass laws that prevent ACVs from being used in certain locations, during certain hours, and in certain ways. A current example of this type of law is London's congestion charge, which limits when drivers are permitted to operate in the core area of the city.[31] An ACV's default programming would obey these laws, as it would for general traffic safety laws. ACV end-users could bypass these restrictions and drive freely anywhere and anytime they please. This is also useful in a navigational context, whereby end-users could traverse prohibited roads to get to their destination faster. This would likely endanger them, since certain roads might be prohibited due to ACVs

---

27. *See* Domenick Yoney, *Tesla Model S owners hack their cars, find Ubuntu,* AUTOBLOG (Apr. 12, 2014 5:00 PM), http://www.autoblog.com/2014/04/12/tesla-model-s-owners-hack-their-cars-find-ubuntu/ (quoting Tesla Motors, Motor Vehicle Purchase Agreement, "You may not, or may not attempt to, reverse engineer, disassemble, decompile, tamper with or engage in any similar activity in respect of a Tesla Vehicle, nor may you permit any third party to do so, save only to the extent permitted by applicable law.").

28. *See* Jack Stewart, *Tesla's Plan to Rule the Auto Industry? In-App Purchases*, WIRED (June 10, 2016, 7:00 AM), https://www.wired.com/2016/06/teslas-plan-rule-auto-industry-app-purchases/all/1. ("This raises the possibility of a black market for hacks to enable these features at no cost. Who'll be the first to jailbreak a Tesla?").

29. *See* Symposium, *Criminal Liability Issues Created by Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1157, 1160 n.8 (2012), http://digitalcommons.law.scu.edu/lawreview/vol52/iss4/2128.

30. Alex Davies, *Audi's Self-Driving Car Hits 150 MPH on an F1 Track*, WIRED (Oct. 24, 2014), https://www.wired.com/2014/10/audis-self-driving-car-hits-150-mph-f1-track/all/1.

31. *See* Mayor of London, *Congestion Charge Factsheet*, TRANSPORT FOR LONDON (June 2014), http://content.tfl.gov.uk/congestion-charge-factsheet.pdf.

being not technically able to navigate them. The incentive remains, however, as it's theoretically possible for an end-user to upload additional software that could render such "impassable" roads traversable.

In addition to bypassing prohibited driving areas, jailbreaking could also help owners disable safety features. ACVs at varying degrees of autonomy will require alerting drivers to resume control when road conditions are no longer fit for the vehicle to drive itself.[32] Some manufacturers have already contemplated how such warning systems would operate in ACVs.[33] Jailbreaks would allow circumventing such features.

One reason to jailbreak is to disable GPS location tracking, namely to protect privacy (assuming such tracking is not critical to vehicle functioning).[34] Most, if not all, ACVs will track location information, and some people fear that companies like Google will take advantage of this personal data for unwanted purposes.[35] Targeted advertising is the most common, if somewhat innocuous, reason.

Disabling location tracking has purposes besides privacy, such as avoiding law enforcement, which could theoretically be able to send a signal to an ACV to bring the vehicle to a safe stop at a given location.[36] This type of capability may or may not be legal under the Fourth Amendment, but if it is ruled to be legal within the ACV traffic stop context, end-users could be given the tool to disable it.[37]

In a similar vein, jailbreaks could allow end-users to defeat forensic "black-box" crash data recorders. Some legislation already requires ACV OEM's to store user-related data recorded in the moments before a crash,

---

32. The 2016 death of Joshua Brown in his Tesla Model A was the first recorded instance of the importance of alerting human drivers to when road conditions are unsuitable for autonomous driving, and more importantly, of educating drivers to take heed of such safety alerts. *See* Rachel Abrams & Annalyn Kurtz, *Joshua Brown, Who Died in Self-Driving Accident, Tested Limits of His Tesla*, N.Y. TIMES (July 1, 2016), http://www.nytimes.com/2016/07/02/business/joshua-brown-technology-enthusiast-tested-the-limits-of-his-tesla.html.

33. "GM's monitoring system has facial recognition software that can detect if a driver is falling asleep or not paying attention . . . If so, the system issues alerts: a red visual display telling a driver to take control followed by a seat vibration and then a recorded audio message. If drivers ignore all those, GM's OnStar system will communicate with the driver." David Shepardson, *U.S. letter reveals details of GM self-driving vehicle system*, REUTERS (Nov. 28, 2016), http://www.reuters.com/article/us-gm-selfdriving-idUSKBN13N2CY.

34. Adrienne Lafrance, *How Self-Driving Cars Will Threaten Privacy*, ATLANTIC (Mar. 21, 2016), https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/.

35. Ellen P. Goodman, *Self-driving cars: overlooking data privacy is a car crash waiting to happen*, GUARDIAN (June 8, 2016), https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security.

36. Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 665 (2015), h8p://scholarship.law.umn.edu/mjlst/vol16/iss2/3.

37. *See* United States v. Jones, 132 S. Ct. 945, 565 U.S. (2012); *See also* Riley v. California, 573 U.S. (2014).

creating digital forensic proof when accidents occur, for legal and insurance purposes.[38] ACV jailbreakers could theoretically disable this feature, allowing one to wipe this type of evidence.

In the context of TNCs and publicly or privately operated fleets of connected vehicles – assuming that individually owned vehicles could join fleets or "platoons"[39] – jailbreaking could allow for "queue prioritization". A jailbroken ACV would be able to join a platoon or somehow gain an unfair advantage when joining a network, prioritizing itself over other ACVs.

One incentive stems from an ACV manufacturer preventing the vehicle from being used as part of a third-party TNC (i.e. a fleet, discussed *supra*). Indeed, Tesla Motors has announced that their full self-driving capability will be available to consumers only on the condition that "using a self-driving Tesla for car sharing and ride hailing . . . for revenue purposes will only be permissible on the Tesla Network."[40] This is a classic example of imposing Digital Rights Management (DRM) onto vehicle software. In electronics and software, DRM is an oft-cited reason for circumvention, and the legality of such circumvention is governed by the copyright system.

Another incentive to jailbreak would be to have control over OEM software updates. Some end-users might balk at an OEM's "permission-less innovation", and be skeptical at their deployment of new services and applications. In the smartphone jailbreaking context, this often occurs because certain software updates create incompatibilities with older applications that end-users still want access to.

Perhaps the most intriguing (and terrifying) reason to jailbreak an ACV is to modify "crash-optimization algorithms".[41] Such algorithms are the way OEM's would determine who or what an ACV would hit if presented with a no-win or catch-22 scenario.[42] This obviously leads to weighty ethical and

---

38. *See e.g.*, Cal. Veh. Code § 38750(c)(1)(G) (2014).

39. "Platooning" is a transportation system that "links vehicles in a high-efficiency group, [bumper-to-bumper] like a train without the train tracks". Stephen Shankland, *Platooning: The Future of Freeways is Lining Up,* CNET (Sept. 3, 2013, 8:44 AM), https://www.cnet.com/news/platooning-the-future-of-freeways-is-lining-up/.

40. Jonathan Gitlin, *Don't Plan on Using Your Autonomous Tesla to Earn money With Uber or Lyft,* ARSTECHNICA (Oct. 20, 2016, 8:47 AM), http://arstechnica.com/cars/2016/10/dont-plan-on-using-an-autonomous-tesla-to-earn-money-with-uber-or-lyft/.

41. *See* Jeffrey K. Gurney, *Crashing into the Unknown: An Examination of Crash-Optimization Algorithms Through the Two Lanes of Ethics and Law*, 79 ALBANY LAW REVIEW 83, 185-86 (2016).

42. *See id.* at 186. (citing *Robot Ethics: Morals and the Machine*, ECONOMIST (June 2, 2012), http://www.economist.com/ node/21556234 ("[A]utonomous machines are bound to end up making life- or-death decisions in unpredictable situations."); *The Robot Car of Tomorrow*, *supra* note 5 ("Some road accidents are unavoidable, and even autonomous cars can't escape that fate."); Jason Millar, *An Ethical Dilemma: When Robot Cars Must Kill, Who Should Pick the Victim*?, ROBOHUB (June 11, 2014), http://robohub.org/an-ethical-dilemma-when-robot-cars-must-kill-who- should-pick-the-victim/ ("We are moving closer to having driverless cars on roads everywhere, and naturally, people are starting to wonder what kinds of

legal implications.[43] A jailbroken ACV could theoretically override these algorithms, prioritizing the lives of vehicle occupants over those in harm's way.[44]

C. *Automotive Electronics and Circumvention*

The electronic innards of motor vehicles have been roughly the same for several decades.[45] Most mechanical components in a modern automobile have embedded electronic control units ("ECUs") that govern their operation and connect them to the rest of a vehicle's systems and subsystems.[46] ECUs communicate with one another via a controller area network (CAN).[47] This creates a type of "thinking nervous system" that can function without a centralized "brain". This eliminates the need for a central host computer to coordinate all operations, as each ECU is able to input and output data to other ECUs and function accordingly.[48] Jailbreaking cannot take place under this type of system.

ACVs differ from this paradigm of automotive electronics because they must include some type of central computer that coordinates all the activities of a vehicle's various subsystems. Such a computer requires a centralized software "brain" to execute autonomous functions.[49] This is the vehicle op-

---

ethical challenges driverless cars will pose. One of those challenges is choosing how a driverless car should react when faced with an unavoidable crash scenario.").

43. *See id.* at 185. (citing Patrick Lin*, Why Ethics Matters for Autonomous Cars*, in AUTONOMES FAHREN 69, 72 (2015) (stating that society will want autonomous vehicles to minimize harm when faced with an unavoidable accident).

44. *See* Kelsey D. Atherton, *MIT Game Asks Who Driverless Cars Should Kill,* Popular Sci. (Oct. 4, 2016), http://www.popsci.com/mit-game-asks-who-driverless-cars-should-kill. (According to an ongoing experiment conducted by M.I.T., dubbed "The Moral Machine," public opinion is split on whether to prioritize a passenger or pedestrian in such scenarios).

45. WILLIAM B. RIBBENS, UNDERSTANDING AUTOMOTIVE ELECTRONICS 3 (6th ed. 2003) (Electronics embedded into automotive components started in the 1970s, when "the introduction of government regulations for exhaust emissions and fuel economy" necessitated better control of the engine than was possible with existing methods, and with "the development of relatively low cost per function solid-state digital electronics.").

46. *See* NAT'L INSTRUMENTS WHITE PAPER, *ECU Designing and Testing using National Instruments Products,* (Nov. 7, 2009), http://www.ni.com/white-paper/3312/en/ (explaining that ECUs are the "brain" of each component they are embedded onto – receiving real-world data via sensors, holding that data in memory and processing it based on logic, and manipulating the component's actuators (i.e., valves, motors, etc.)).

47. NAT'L INSTRUMENTS WHITE PAPER, *Controller Area Network (CAN) Overview* (Aug. 1, 2014), http://www.ni.com/white-paper/2732/en/.

48. ECU and CAN circumvention have traditionally been used to override a vehicle's default speed limit, pollution control limits, tweak engine and/or turbocharger performance, manipulate dashboard indicators, and extend infotainment functionality, among other purposes.

49. Glancy, *supra* at note 37, at 639 (citing INT'L TRANSP. FORUM, ORG. FOR ECON. COOPERATION & DEV., AUTOMATED AND AUTONOMOUS DRIVING: REGULATION UNDER UNCERTAINTY 11-12 (2015), http://www.internationaltransportforum.org/pub/pdf/15CPB_AutonomousDriving.pdf; NAT'L SCI. FOUND., *Programming Safety into Self-Driving Cars,* (Feb. 2,

erating system, built atop the existing ECU/CAN architecture, which creates the "surface" through which a jailbreak will penetrate. Within milliseconds, this brain receives the sensor and actuator data from mechanical components, makes decisions, and executes commands back to those parts.[50]

Some companies, like Tesla Motors, have already created their own vehicle operating system (based on the Ubuntu Linux platform).[51] This operating system is essentially no different than the ones that operate on desktop computers and mobile devices.[52]

The Tesla architecture is highly relevant because it has already been jailbroken, and a minor controversy occurred as a result.[53] A curious owner in France was able to gain access to the vehicle operating system and shared his methods on an online enthusiast forum.[54] The press used the very term 'jailbreaking' when reporting on the circumvention.[55] The owner later reported that the company found out about his circumvention and contacted him, threatening to void his warranty if he did not cease his activities. The owner never reported any follow-ups by Tesla, other than the initial censure.

2015), http://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=134033&org=IIS (introducing algorithms designed to incorporate adequate safety controls in semi-autonomous vehicles)) ("An autonomous car will rely on highly sophisticated computer processing to integrate and analyze internal vehicle operational data and roadway sensor data and then to determine which automated controls to activate and trigger them. Artificial intelligence integrates internal vehicle operational and external roadway environment inputs.").

50. James Morra, *NXP Builds Computer Engine for Self-Driving Cars*, ELECTRONIC DESIGN (May 17, 2016), http://electronicdesign.com/microprocessors/nxp-builds-computer-engine-self-driving-cars (describing the BlueBox autonomous vehicle platform as "a central computer engine fueled by the bits streaming in from sensors around the vehicle. It knits together all the different sensors found in autonomous cars, including radars, cameras, and Lidar systems.").

51. Nikki Gordon-Bloomfield, *Owners Hack Tesla Model S Electric Car: Tesla Politely Asks Them to Stop,* TRANSPORT EVOLVED (Apr. 8, 2014), https://transportevolved.com/2014/04/08/owners-hack-tesla-model-s-electronic-car-tesla-politely-asks-stop/ ("Ubuntu Under the Hood . . . Those who have looked claim the Model S' operating system seems to be based on a special variant of Ubuntu, a Debian-based Linux operating system.").

52. Jason Torchinsky, *The Tesla Model S Is Basically a Good Looking IT Department on Wheels*, JALOPNIK (Apr. 4, 2014), http://jalopnik.com/the-tesla-model-s-is-basically-a-good-looking-it-depart-1558372928 ("It's really odd just how, well, normal all this feels — it's just like any home or office network. They're using it in some interesting ways — for example, the current song playing artwork is being served to the center large display simply like normal web traffic . . . He even managed to get Firefox running on both the center screen and the dash cluster screen.").

53. *Tesla Model S Ethernet Network Explored, Possible Jailbreak in the Future?*, DRAGTIMES (Apr. 4, 2014), http://www.dragtimes.com/blog/tesla-model-s-ethernet-network-explored-possible-jailbreak-in-the-future ("All of this technology certain [sic] brings up the question as to when and if Tesla's internal systems will be hacked and jailbroken to allow 3rd party applications to run on the large 17? touchscreen."); Torchinsky, *supra* note 52.

54. nlc, *Successful Connection on the Model S Internal Ethernet Network,* TESLA MOTORS FORUM (Mar. 2, 2014), https://teslamotorsclub.com/tmc/threads/successful-connection-on-the-model-s-internal-ethernet-network.28185/#post-595400.

55. *E.g.,* Torchinsky, *supra* note 53.

This indicates how ACV makers could posture similarly to smartphone makers when it comes to jailbreaking – namely that companies make veiled threats to void warranties or similar contractual invocations.

More recently, an ACV startup has decided to open source its vehicle operating system[56], which would allow drivers to load their own custom autonomous driving software without having to circumvent an existing system.[57] These open source alternatives demonstrate not only that vehicle operating systems are becoming commonplace, but that third-party alternatives are collaboratively developed and shared widely.

III. Copyright Liability

The legality of circumventing digital products is determined by an intellectual property regime, Section 1201 of the Digital Millennium Copyright Act. ACV jailbreaks fall under this law, and those involved in jailbreaking could thus incur civil and criminal liability, barring a special exemption permitting certain cases of circumvention for the public interest. The pursuit of legal action is at the discretion of ACV companies, the outcome of which is likely to vary widely due to the courts' lack of a uniform interpretation of the statute. It is also possible that Section 1201 may be overturned entirely by the time ACVs are widespread.

As mentioned previously, ACVs jailbreaks are a type of software circumvention, and since software code is copyrightable, their legality is governed by copyright law,[58] including the Digital Millennium Copyright Act ("DMCA").[59] For this reason, those who develop[60], distrib-

56. Tim Higgins, *George Hotz's Startup Gives Away Semiautonomous-Driving Software,* Wall St. J., (Nov. 30, 2016), http://www.wsj.com/articles/george-hotzs-startup-gives-away-semiautonomous-driving-software-1480548039.

57. The open source ACV OS can be found at https://github.com/commaai/openpilot. The developer describes its capabilities as "perform[ing] the functions of Adaptive Cruise Control (ACC) and Lane Keeping Assist System (LKAS) for Hondas and Acuras. It's about on par with Tesla Autopilot at launch, and better than all other manufacturers."

58. The Copyright Act, 17 U.S.C. §§ 101-810 (1976) (The Copyright Act treats software code as a literary work, which is protected under 17 U.S.C. § 102, granting protection to "original works of authorship fixed in any tangible medium of expression . . . from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.").

59. *See* Off. of Legal Educ. Exec. Office for U.S. Attorneys, *Prosecuting Intellectual Property Crimes* 235 (4th ed. 2013), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/prosecuting_ip_crimes_manual_2013.pdf ("Congress intended Title I of the DMCA to apply to copyrighted works that are in digital format and thus could easily and inexpensively be accessed, reproduced, and distributed over the Internet without the copyright owner's authorization.") [hereinafter Prosecuting IP Crimes].

60. Jailbreak developers are typically product enthusiasts with the requisite skills in software development and automotive electronics. *See* Yukari Iwatani Kane, *The iPhone 3GS Hacking Debate,* Wall St. J. (July 6, 2009, 9:02 PM), http://blogs.wsj.com/digits/2009/07/06/the-iphone-3gs-hacking-debate/ (discussing how early iPhone jailbreaks were developed by "the iPhone Dev Team, a loose-knit but exclusive group of highly-skilled technologists.").

ute[61], install[62], or use an ACV jailbreak, barring a statutory exemption, would infringe the software copyright of ACV manufacturers and/or suppliers.

A. *DMCA § 1201*

DMCA Section 1201(a), otherwise known as the "anti-circumvention provision", applies to two variants of "digital lock" technology: access-control measures ("ACMs") and copy-control measure ("CCMs"), collectively known as TPMs.[63] ACMs limit *access* to protected works using such controls as passwords and encryption, while CCMs limit the ability for users to *copy* said works after they have already gained access to them. Section 1201 expressly prohibits the circumvention of ACMs, but not of CCMs. Since jailbreaking circumvents the ACV manufacturer's "digital lock" on the operating system, those who develop, distribute, install, or use an ACV jailbreak would infringe Section 1201.

The law does not stop at prohibiting the creation and use of circumvention tools — it also prohibits the trafficking of them, regardless of whether such tools lead another party to circumvent an ACM or CCM.[64] These so-called "anti-trafficking provisions" make it illegal to traffic in both ACMs and CCMs, even though actual circumvention of CCMs is permitted.[65]

ACV jailbreaks would violate these provisions outright, because they would necessitate circumventing an ACV's ACMs and CCMs, which is exactly what Section 1201 addresses. In addition, the marketing and distribution of such circumventions ("trafficking", per the statute's language) would also plainly violate this law. It is only by statutory exemption that ACV jailbreaks might pass muster.

---

61. In most instances, jailbreaks are not created for commercial gain, and are often part of an open-source development project in which anyone can contribute to the freely available codebase. *See* John Koetsier, *Jailbreaking iOS 7: A crowdfunded 'device freedom prize' for the first open source exploit*, VENTUREBEAT (Dec. 4, 2013, 5:29 PM), http://venturebeat.com/2013/12/04/jailbreaking-apples-ios-7-now-theres-a-crowdfunded-device-freedom-prize-for-the-first-open-source-exploit/ (quoting the Device Freedom Prize group, "We strongly believe that users should have the freedom to control their devices . . . We want an open source jailbreak for iOS 7.").

62. *See, e.g.,* US Copyright Office Study: Software-Enabled Consumer Products, at Fn. 173: Auto Care Ass'n Initial Comments at 5 (stating that "vehicle parts manufacturers and servicers have been sued and threatened with suit for copyright infringement merely for engaging in repairs of software-controlled parts"); *see also* Tr. at 49:04-10 (May 18, 2016) (Shaun Bockert, Dorman Products, Inc.) (referencing lawsuit involving Dorman, see Am. Compl. and Jury Demand, General Motors LLC v. Dorman Prods., Inc., No. 2:15-cv-12917 (E.D. Mich. Aug. 18, 2015)).

63. 17 U.S.C. § 1201(b)(1) and 17 U.S.C. § 1201(b)(2).

64. *See* Davidson & Assocs. v. Jung, 422 F.3d 630, 640 (8th Cir. 2005); *See also* Universal City Studios v. Corley, 273 F.3d 429, 440-41 (2nd Cir. 2001).

65. 17 U.S.C. § 1201(a)(2) and 17 U.S.C. § 1201(b)(1).

Since Section 1201 enables copyright owners to lock down devices to support only certain software, services, and geographic regions, it is often blamed for stifling "both innovation and [aftermarket] competition in technology and entertainment markets", as well as limiting free expression, jeopardizing fair use, and impeding security research.[66] The market for ACVs and their software is no exception. But Congress wanted to ensure that the general public has the tools to make fair and non-infringing uses of copyrighted works, while the making of infringing copies of a work are already addressed in other areas of U.S. copyright law.[67] Thus, the Library of Congress ("Library") grants exemptions for certain categories of circumvention that are found to be in the public interest.[68] ACV jailbreaks may potentially be granted such an exemption.

B. *Statutory Exemptions*

The Section 1201 rulemaking process was designed to place the DMCA "in accord with the constitutional directive of the Copyright Clause and fair use doctrine codified in 17 U.S.C. § 107."[69] It is a mechanism that aims to reconcile the competing interests of copyright holders and the general public, namely ordinary consumers, educators, researchers, and competitors.[70] These interests have been at the heart of the smartphone jailbreaking debate, and would be weighed similarly in a determination of an exemption for ACV jailbreaks.

The triennial rulemaking "is a highly visible and public process, commenced every three years". Members of the public propose potential exemptions, and they are evaluated through "several rounds of public notices, written comments, and public hearings. The Librarian of Congress then adopts exemptions based upon the recommendation of the Register of Copyrights—who in turn receives input from the public and from the National Telecommunications and Information Administration ("NTIA")."[71]

1. "Lawful modification"

In October of 2015, after an exhaustive notice and comment period overseen by the Register of Copyrights ("Register"), the Library granted exemptions ("2015 Exemptions") for the circumvention of "motorized land vehicle

66. Maryna Koberidze, *The DMCA Rulemaking Mechanism: Fail or Safe?*, 11 WASH. J. L. TECH. & ARTS 211, 224 (Fall 2015) (citing S. Rep. No. 105-190, at 12 (1998)).

67. *Id.* at 230

68. *Id.* at 227.

69. *Id.* at 228.

70. Exemptions are valid for only three years. At the start of each rulemaking cycle, the public is invited to submit proposals to the Register of Copyrights, who then hosts a process of hearings and public comments, after which the final rule is put forward by the Register and issued by the Librarian of Congress.

71. U.S. COPYRIGHT OFF., *Understanding the Section 1201 Rulemaking*, at 1, https://www.copyright.gov/1201/2015/2015_1201_FAQ_final.pdf.

[software]" for the purposes of "lawful modification" and "good-faith security research."[72] These provisions are critical to understanding future exemptions potentially granted for ACV jailbreaks. Proponents included the Electronic Frontier Foundation ("EFF") and the Intellectual Property & Technology Law Clinic of the University of Southern California Gould School of Law. It was opposed by the Alliance of Automobile Manufacturers, Association of Global Automakers, Eaton Corp., General Motors, John Deere, and the Motor & Equipment Manufacturers Association.

The first exemption is for "lawful modification", justified as a non-infringing activity and as a matter of fair use, specifically for,

> "Computer programs that are contained in [ECUs] and control the functioning of a motorized land vehicle such as a personal automobile [or] commercial motor vehicle, except for computer programs primarily designed for the control of telematics or entertainment systems for such vehicle, when circumvention is a necessary step undertaken by the authorized owner of the vehicle to allow the diagnosis, repair or lawful modification of a vehicle function;[73] and where such circumvention does not constitute a violation of applicable law, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency. . .".[74]

Proponents wanted the rule to allow for "aftermarket personalization, modification, or other improvement . . . such as enhancing a vehicle's suspension or installing a gear with a different radius", but this was rejected in the final rule.[75] This is indicative of the Library's view of automotive software circumvention, namely that it should only be allowed for a very narrow set of circumstances (as is enumerated in the final rule). For example, telematics and entertainment systems were specifically excluded from the exemption. Based on this ruling, we can extrapolate that any proposal for ACV jailbreaking would likely be rejected, and for two key reasons.

First, a jailbreak would allow for too broad a range of activities, falling outside the narrow scope of purposes the current exemptions accommodate. It is one thing to circumvent a few ECUs related to a specific repair or research objective, it is another to circumvent a whole-car OS, granting access to all functions. Jailbreaking allows for such frivolous capabilities as

---

72. *See,* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,955 (Oct. 28, 2015) (37 C.F.R. § 201.40), http://federalregister.gov/a/2015-27212 [hereinafter "2015 Exemptions"].

73. Opponents to this exemption argued that it "would not facilitate non-infringing uses, and was unnecessary in any event because vehicle owners have alternative options, such as manufacturer-authorized repair shops and tools." *Id.* at 28.

74. *Id.*

75. 2015 Exemptions, *supra* note 72, at 65956.

programming the ACV to execute "donuts" without requiring human control (which tends to be difficult for an average driver to perform).[76]

Second, while the current exemption acknowledges the safety risks inherent in the circumvention of motor vehicles (specifying that "security research must be conducted in a controlled setting designed to avoid harm to individuals or the public"), these risks would not compare to those presented by ACV circumvention.[77]

Probing the question not through the vehicles exemption but through the smartphone jailbreaking exemption (which was granted for the third cycle in a row), the analysis is still not favorable to ACV jailbreaking. The set of activities enabled by smartphone jailbreaking is seen as beneficial to its users with little to no risk of harm posed to others. But the set of activities enabled by ACV jailbreaking and the concomitant harms that could arise would likely be too great for a future Library administration to support.

Also crucial to note is the carve-out for telematics or entertainment systems. As discussed earlier, these systems are often the crux of an automotive circumvention, as demonstrated by the 2014 Jeep Hack and similar examples.[78] However, the Register did not cite that as a concern in her reasoning. She concluded that there was "insufficient evidence demonstrating a need to access such [entertainment and telematics] ECUs", and that "such circumvention might enable unauthorized access to creative or proprietary content."[79] Prioritizing content infringement concerns over safety or security concerns appears odd, and is perhaps a single ray of hope for ACV jailbreaking to be exempted in the future, so long as it somehow "distracts" the Register with other concerns, as occurred here.

The views of the opposition (namely that of automakers, suppliers, and other government agencies) are instructive on the issue of safety. Their position is described by the Register below:

> "The agencies' concerns were focused on potential adverse effects on safety and the environment. For example, EPA explained that vehicle modifications are often performed to increase engine power

76. A "donut" is a vehicular stunt whereby a driver rotates either the front or rear wheels around the polar set of wheels in a continuous motion, leaving concentric circular skidmarks on a roadway.

77. 2015 Exemptions, *supra* note 72, at 65,956.

78. *See* Charlie Miller & Chris Valasek, *A Survey of Remote Automotive Attack Surfaces*, ILLMATICS 15-20, http://illmatics.com/remote%20attack%20surfaces.pdf; *See also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/all/1 ("Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.").

79. 2015 Exemptions, *supra* note 72, at 65,956.

> or boost fuel economy, but that these modifications increase vehicle emissions and thus violate the Clean Air Act."[80]

This was a significant sticking point in the 2015 rulemaking process, and there was a high level of crosstalk between the Library and these agencies to settle the issue.[81] From this we can infer that any future rulemaking around ACV jailbreaking would necessarily involve relevant agencies such as the Department of Transportation ("DOT") and the Environmental Protection Agency ("EPA"), outside of any other enforcement issue discussed further in this paper.[82]

2. "Good-faith security research"

The second of the relevant 2015 Exemptions permits "good-faith security research", specifically,

> "for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, when such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."[83]

The automotive industry vehemently and unsuccessfully opposed this exemption, citing the malicious use of such research by "bad actors" to hack into vehicles. But the interest in security research outweighed the downsides, with the Register finding that "legitimate security research has been hindered by TPMs that limit access to those programs."[84]

The Register went on to articulate two other significant issues with the security research exemption: the application of research findings and the proper treatment of their disclosure. In the first instance, it was acknowledged that "the interests of the manufacturer and the public may both be affected by the nature and timing of disclosure of software flaws".[85] In the second, it was acknowledged that ". . .information derived from the research

---

80. *Id.*

81. *See id.*

82. There is no reason to believe otherwise – EPA's concerns were unequivocally validated when over one month before the 2015 Exemptions were granted, a massive scandal erupted over Volkswagen admitting that 11 million of its vehicles "were equipped with software that was used to cheat on emissions tests." *See* Gates, et al., *Explaining Volkswagen's Emissions Scandal*, N.Y. Times (July 19, 2016), http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html.

83. 2015 Exemptions, *supra* note 72, at 65956.

84. *Id.*

85. *Id.*

activity be used primarily to promote the security or safety of the devices containing the computer programs on which the research is conducted, or of those who use those devices."[86] These are important provisions, and ones that make sense for today's vehicles and ACVs in the future.

Applying the security research exemption to ACV circumvention would be theoretically possible under the justification that a large amount of ACV research and testing takes place in designated secure settings (either private corporate facilities or those of educational institutions), and is conducted by avid professionals that would properly disclose flaws.[87] Since ACVs necessarily require whole-car OSs, circumvention technology may be exempted for this narrowly tailored use. This of course says nothing of consumer installations of jailbreaks, which would presumably be prohibited under any scenario.

3. Returning to the 2015 Exemptions' smartphone jailbreaking provision, the Library exempted

> "Computer programs that enable smartphones . . . to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smartphone or device, or to permit removal of software from the smartphone or device."[88]

This is sensible for the fragmented world of smartphones and cellular networks, but is it for the world of ACVs? We know that connected vehicles will function similarly to smartphones and cellular networks, with manufacturers enabling connectivity between their own vehicles (or to allied manufacturers' vehicles) and to roadway infrastructure, but it is not necessarily the case that all vehicles in the U.S. fleet will connect with one another.[89] ACV jailbreaks could enable such interoperability, as jailbreaks do for smartphones, and that logic leans in favor of a narrowly tailored ACV jailbreak exemption. Whether such jailbreaks could be "lawfully obtained" is a separate question, and one that is unlikely to weigh in favor of this category of circumvention.

Jailbreaking of any machine or device for purposes other than those permitted by the 2015 Exemptions would immediately trigger the liability enumerated in DMCA §1201, which carries civil and criminal penalties. Given

86. *Id.*

87. The University of Michigan contains one such facility, the Mobility Transformation Center, whose homepage may be found at M City, http://www.mtc.umich.edu/.

88. 2015 Exemptions, *supra* note 72, at 65953.

89. One such "alliance" is the Crash Avoidance Metrics Partnership ("CAMP"), a partnership between Mercedes-Benz, General Motors, Toyota, Nissan, Volkswagen, Hyundai-Kia Motors, Honda, and Ford. *See* Rachel King, *Automakers Tackle the Massive Security Challenges of Connected Vehicles*, WALL ST. J. (June 25, 2015), http://blogs.wsj.com/cio/2015/06/25/automakers-tackle-the-massive-security-challenges-of-connected-vehicles/.

the nature of the 2015 Exemptions, specifically around motor vehicles, it is unlikely for ACV jailbreaks to be granted an exemption in the future, except perhaps for the narrowly tailored purpose of private security research and interoperability.

C. *Civil and Criminal Ramifications*

In the absence of a Section 1201 exemption, ACV jailbreaks will incur infringement liability. The statute provides civil remedies to copyright holders who may at their discretion choose to litigate under the statutory right of action against unwanted circumvention of their works.[90] It also creates criminal offenses and penalties to be prosecuted at the discretion of the Department of Justice ("DOJ").[91]

In civil actions, damages constitute both "actual damages suffered by the party as a result of the violation" as well as "any additional profits of the violator".[92] Statutory damages are also available to plaintiffs.

In criminal cases, penalties are not trivial, with fines up to $500,000 or imprisonment for up to 5 years, for the first offense.[93] It only gets worse from there. However, educational institutions like the ACV research facilities discussed above are exempted from these offenses.

Criminal actions require the government to establish that the defendant willfully circumvented an ACM of a copyrighted work for "commercial advantage or private financial gain."[94] The type of harm that ACV jailbreaks could potentially cause (to persons or property) is not addressed in the criminal liability section of the statute, leaving that to judicial interpretation or for a separate liability regime. Regardless, an ACV jailbreak is no different than any other circumvention discussed in the DMCA, and barring an exemption would still constitute a criminal offense regardless of the potential for harm to persons or property.

D. *Discretion to Litigate*

It is at the discretion of copyright holders to pursue action against an alleged circumventor. In some instances, copyright holders choose *not* to file suit, as is the case with Apple, Inc.'s treatment of the development commu-

90. "Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation." 17 U.S.C. § 1203 (2017). Courts have the power to "grant temporary and permanent injunctions," "order the impounding . . . of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation," "allow the recovery of costs by or against any party," and "order the remedial modification or the destruction of any device or product involved in the violation." 17 U.S.C. § 1203 (2017).

91. 17 U.S.C. § 1204 (2017).

92. 17 U.S.C. § 1203(c)(1) (2017).

93. The first case where the DOJ prosecuted a defendant for §1201 violations was *U.S. v. Elcom, Ltd.*, 203 F.Supp.2d 1111 (N.D. Cal. 2002).

94. Prosecuting IP Crime, *supra* note 59, at 326.

nity that for years has been jailbreaking the iPhone's iOS operating system.[95] Despite being in a constant arms race with these circumventors, they have turned a blind eye and never legally threatened them.

There are many reasons for this, of which the same would apply to ACV jailbreaking. First, through the process of developing a circumvention, jailbreaking communities indirectly assist with the detection of bugs. As is the case in unofficial cybersecurity research, the goodwill of these communities often leads to good faith disclosures to manufacturers.[96] As mentioned earlier, Apple has even thanked jailbreakers (in the release notes of a software update) for finding a bug in iOS. Given the heavily software-driven nature of ACVs, detection and disclosure of such security vulnerabilities would serve an important function.[97]

Second, because courts have been unpredictable in their application of DMCA §1201, companies may be hesitant to pursue capricious litigation, which drains time and resources and could lead to negative legal precedent.[98] Third, companies must weigh the potential adverse publicity or perception of anticompetitive behavior that would likely result from litigation.[99] There is also a societal conception of "ownership" over a consumer product that would be violated, leading to further negative publicity.[100] A company in the automotive industry—an industry core to the nation's sense of pride and whose products are a daily fixture of peoples' lives—would feel the reputational consequences arising out of litigation against their own enthusiasts.

Another incentive for ACV manufacturers to turn a blind eye is to increase customer satisfaction and perhaps capture new customers. Customers in this market will want access to newer software-enabled features, but it might be the case that even though official over-the-air software upgrades can technically deliver these improvements, they might not be distributable

---

95. *See* Yoney, *supra* note 27.

96. Indeed, this is already starting to happen in the automotive sphere, thanks to the 2015 DMCA Exemptions. Andy Greenberg, *It's Finally Legal To Hac, Your Own Devices (Even Your Car)*, WIRED (Oct. 31, 2016), https://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/all/1 ("Since [General Motors] launched a vulnerability disclosure program in January that offered some assurance it wouldn't sue helpful hackers, it's received hundreds of reports of security vulnerabilities in its cars.").

97. This is very common in the information technology arena. *See* U.S. COPYRIGHT OFF., *Software-Enabled Consumer Products* at 42-45 (Dec. 15, 2016), https://www.copyright.gov/policy/software/software-full-report.pdf. "For example, Google has offered a 'Vulnerability Reward Program' since 2010 to encourage security researchers to identify technical vulnerabilities in its system, and it offers $500 to $100,000 for researchers who identify qualifying bugs through its 'Chrome Reward Program.' Other companies such as Facebook, Microsoft, and Mozilla offer similar security research rewards programs." *Id.* at 45.

98. *See* Eric Stevens, *Fair Competition or Unlawful Circumvention?: The DMCA and Product Aftermarkets,* FOR THE DEFENSE at 53 (Jan. 2016), http://www.poynerspruill.com/publications/Documents/FTD-1601-Stevens.pdf.

99. *Id.* at 56.

100. *Id.*

due to pending regulatory approval. Permitting jailbreaks allows customers to access new features without the manufacturer running afoul of regulations.[101]

Conversely, there are plenty of reasons for ACV manufacturers and/or suppliers to move forward with assertive enforcement actions, chiefly that of deterring circumventions that could potentially lead to serious harms. A jailbroken smartphone, outside of damaging itself, cannot cause extrinsic harm. In contrast, an accident caused by a jailbroken ACV could lead to property damage, personal injury, or death. It might even be the case that ACV manufacturers and/or suppliers are imposed some type of duty to enforce Section 1201.

E. *Common Law Interpretations*

In the seventeen years since the DMCA was enacted, there has yet to be an overarching common law interpretation of Section 1201. Some cases have been very favorable toward copyright holders, and others have treated them less so. Some have entertained First Amendment challenges to the claims, and others have discarded them outright. Like the rest of U.S. copyright law, the result is a hodgepodge of rulings that are difficult if not impossible to reconcile.

1. Cases at the Northern District of California

The Northern District of California is home to numerous technology companies, and thus has hosted many of the important cases in this area of the law. But even within this single jurisdiction, there are conflicting interpretations. In *321 Studios v. Metro Goldwyn Mayer Studios, Inc.* (2004), the court ruled that DVD copying software violated § 1201. It further concluded that the anti-circumvention provisions of the DMCA were constitutional. The court ruled similarly in another DVD copying software case, *Realnetworks, Inc. v. DVD Copy Control Assn., Inc.* (2009). While useful in establishing the inconsistency of rulings between the Northern District versus other jurisdictions, these cases differ factually from ACV circumvention. DVD copying concerns unauthorized duplication, not the modification of operating systems to expose unauthorized *functionality*.

The same court, however, issued a mere slap on the wrist in a case much more germane to ACV jailbreaking. *Sony Computer Entertainment America, Inc. v. Hotz* (2011). There, a hacking group circumvented the Sony PlayStation video game console's TPMs to jailbreak the operating system. The modified OS enabled new functionality such as backing up games for diskless play, playing pirated games, the support of different video formats, and the ability to run other software and applications. The case ended in a temporary restraining order that forbade defendants from distributing the jail-

101. *See* Stewart, *supra* note 28.

break, helping or encouraging others to jailbreak, and trafficking the information they learned during their circumvention.

The court was also favorable to the defendant in *United States v. Elcom, Ltd. and Dmitry Sklyarov* (N.D. Cal. 2002), a case famous for being the DOJ's first criminal prosecution of an individual §1201 defendant. There, Sklyarov sold software that removed restrictions from Adobe Portable Document Format ("PDF") files, such that users could freely download, read, and archive PDF-protected eBooks. The charges were dropped and Sklyarov and Elcomsoft were found not guilty. This case is more akin to the DVD copying cases in that the circumvention was not designed to expose additional functionality of a software program.

2. Cases Elsewhere in the Country

At the Ninth Circuit, mixed results were shown when the court in *MDY Industries, LLC v. Blizzard Entertainment, Inc.* (9th Cir. 2011) ruled in favor of defendants for both ACM circumvention and trafficking claims but not for a separate ACM circumvention claim. There, a company was sued for creating an application that allowed the players of a video game to automate playing the game to level-up players' characters. This case does not bear directly on ACV jailbreaking, since it is only about a software circumvention that hastens the arrival of features that are already available if one plays the levels of the game.

In another major case heard in Illinois, *Agfa Monotype Corp. v. Adobe Systems, Inc.* (N.D. Illinois 2005), the defendants enjoyed a favorable outcome over their circumvention of copyrighted fonts embedded in PDF files. There, the court held that defendant did not violate the DMCA because the TPM did not effectively control access to the fonts. Again, this case is useful in explaining the chaotic DMCA rulings across the nation, but bears little on ACV jailbreaking.

Meanwhile, defendants were treated fairly in another seminal case heard at the Federal Circuit, *Chamberlain Group, Inc. v. Skylink Technologies, Inc.* (2004).[102] There, creators of a universal transmitter for garage doors circumvented a manufacturer's "rolling code" so that transmitters could be used across a variety of doors. Defendants were held not to have violated § 1201. The Federal Circuit decision is in stark contrast to New York, where courts that have heard some of the largest cases in this area of law have repeatedly ruled in favor of plaintiffs. *Universal City Studios, Inc. v. Reimerdes* (S.D.N.Y. 2000); *Universal City Studios, Inc. v. Corley* (2nd Cir. 2001). In the *Universal* cases, the court held that creators and distributors of DeCSS

102. The Federal Circuit is supposed to hear only patent cases, but sometimes these cases have copyright claims that ride along, bringing copyright cases into their jurisdiction as well, which has led to circuit splits in other areas of copyright law. Federal Courts Improvement Act of 1982, Pub. Law 97-164, 96 Stat. 25 (Apr. 2, 1982), https://www.gpo.gov/fdsys/pkg/STATUTE-96/pdf/STATUTE-96-Pg25.pdf.

(DVD decryption software) violated the DMCA, which was "content-neutral as applied to computer programs".[103] It also held that the defendants' First Amendment rights were not violated by the statute.[104] Again, these cases are relevant due to their role in shaping anti-circumvention law, but do not bear on ACV jailbreaking directly.

It is clear that civil action against ACV jailbreaks will produce widely differing outcomes depending on the jurisdiction. In California, courts will likely rule in favor of jailbreaker(s), or to at least rule favorably for *some* of the claims. Meanwhile, in New York, courts are more likely to rule in favor of plaintiffs. And yet if a suit were brought before the Federal Circuit, it could be a different outcome. Only one jurisdiction has heard a case that bears directly on operating system jailbreaking (N.D. Cal. and the Sony PlayStation case), and it is thus difficult to say how another jurisdiction would treat a case with similar facts, other than how they've ruled on other anti-circumvention cases.

Geography alone is not dispositive to these types of cases, as courts have examined a variety of defenses, which include the following: (1) Library of Congress exemptions; (2) statutory carve-outs for certain nonprofit entities, information security purposes, reverse engineering and technology interoperability, security and encryption research, restriction of minors' access to the Internet, and protection of personally identifying information; (3) First Amendment freedom of express ("chilling effects") challenges based on either "facial" or "as applied" arguments; (4) Fifth Amendment vagueness challenges; and (5) the fair use doctrine of the Copyright Act.[105]

F. *Challenge to § 1201*

Regardless of statutory and judicial interpretations of ACV jailbreaking under Section 1201, it is also possible that by the time ACVs are widespread, the statute will be overturned. Since its inception, cases have challenged its constitutionality on First Amendment grounds, but the statute still stands. This is changing now, with the Electronic Frontier Foundation launching a new First Amendment freedom of expression suit against the U.S. government on behalf of technologists and researchers to overturn Section 1201.[106] EFF argues that "the prospect of costly legal battles or criminal prosecution stymies creators, academics, inventors, and researchers . . . Sec-

103. *See* Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, at 332 (S.D.N.Y. 2000)

104. *Id.* at 346.

105. *See* Prosecuting IP Crimes, *supra* note 59, at 263-79.

106. Electronic Frontier Found, *EFF Lawsuit Takes on DMCA Section 1201: Research and Technology Restrictions Violate the First Amendment* (July 21, 2016), https://www.eff.org/press/releases/eff-lawsuit-takes-dmca-section-1201-research-and-technology-restrictions-violate.

tion 1201 threatens ordinary people with financial ruin or even a prison sentence" when they exercise their First Amendment freedom of expression.[107]

The suit is based on the following key arguments: that certain instances of circumvention, like security research, constitute an antecedent step of free speech (the final step being publishing results of said research), and that those steps are protected by the First Amendment; that the triennial rulemaking process is an unconstitutional speech-licensing regime; that the entirety of § 1201 is an unconstitutional speech-licensing regime.[108]

Were such a challenge to be successful, an entirely new legal mechanism to address circumvention would have to be created, and it is unclear how ACV circumvention would be treated by that regime. It is possible that it would be usurped into an entirely separate ACV law that addresses all of its facets, not just circumvention.

G. *Copyright: An Ill-suited Tool*

It is worth asking why the Copyright Office would be responsible for ACV anti-jailbreaking policies in the first place. Why should copyright policy help regulate motor vehicle safety concerns? The copyright system is fraught with tension: existing provisions of the Copyright Act, agency rulemaking, judicial interpretations, and private-sector efforts, are what is relied upon to maintain balance in the system.[109] It is unwise to use such an unstable system to regulate the complex development of ACVs.

The unique circumstance of ACV jailbreaks, namely that they are a software circumvention with a serious risk of injury or death, would make it sensible for Congress or NHTSA to enact legislation or regulation to address their legality. Such a measure should do so with an eye to DMCA § 1201 and its exemption process, specifically excluding ACV jailbreaks from being exempted in the first place, and circumscribing a narrow set of conditions for which a jailbreak would be legal. It might also specify, for example, that only ACV manufacturers and authorized third parties may modify a vehicle operating system.

---

107. *Id.*

108. "To be sure, in *Eldred v. Ashcroft*, 537 U.S. 186, 219 (2003), the Supreme Court found that Congress has substantial authority to legislate under the Copyright Clause without running afoul of the First Amendment, but that holding was subject to a vital qualification: such legislation must adhere to the 'traditional contours' of copyright. *Id*. at 221. The Court specifically identified the idea/expression dichotomy and fair use as 'built-in First Amendment accommodations' that mark those contours. In *Golan v. Holder*, 132 S. Ct. 873, 890 (2012), the Court renewed its recognition that copyright law embraces the idea/expression dichotomy and fair use as 'speech-protective purposes and safeguards' that, if disturbed, would subject the law at issue to ordinary First Amendment scrutiny. *Id.*" Memorandum in Support of Motion for Prremiminary Inunction on Behalf of Plaintiff at 15, Green v. U.S. Dep't of Justice, No. 16-cv-01492-EGS (D.D.C. Aug. 29, 2016), ECF No. 16, https://www.eff.org/document/green-v-doj-motion-preliminary-injunction.

109. *See* U.S. COPYRIGHT OFF., *supra* note 97, at Fn. 178 (citing Microsoft Initial Comments at 9).

Furthermore, ACV jailbreaking might be deterred entirely by strong state legislation governing the technology generally.

H. *ACV-specific Statutes*

Many states are also in the midst of drafting ACV development statutes that could impose broad criminal liability onto jailbreak-side parties.[110] Legislation in Michigan is one such example.[111] Several bills have been enacted into law, and a few are still in process. One of the passed laws exempts manufacturers from liability if "another person" converts or attempts to convert their motor vehicle into an automated one (and includes provisions for installation and modification of equipment to achieve such ends),[112] indirectly placing such liability on jailbreak-side parties. Two bills in the Michigan State Senate go a step further. One provides that:

> "A person shall not intentionally access or cause access to be made to an electronic system of a motor vehicle to intentionally destroy, damage, impair, alter, or gain unauthorized control of the motor vehicle."

The punishment specified is "imprisonment for life or any term of years".[113] Another specifies that "access[ing] electronic systems of motor vehicle to obtain data or control of vehicle" is a Class A felony punishable by a statutory maximum of life imprisonment. This is as strong a deterrent against jailbreaking as any of the civil and criminal penalties imposed by DMCA § 1203 and 1204.

As the notable autonomous vehicle law scholar Bryant Walker Smith has written regarding this proposed legislation:

> "The primary intent of these bills is, I would hope, to prohibit malicious interference with a vehicle. The broad language of [these bills] goes far beyond any such aim. A literal interpretation would make criminals out of manufacturers that send over-the-air updates to their vehicles, vehicle owners who accept such updates, repair

---

110. Daniel A. Crane, Kyle D. Logue, & Bryce C. Pilz, *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles* at 3 (July 2016) U of Michigan Public Law Research Paper No. 510, U of Michigan Law & Econ Research Paper No. 16-015, https://ssrn.com/abstract=2807059 ("Having previously adopted autonomous vehicle testing regulations, the California Department of Motor Vehicles on December 16, 2015 released its much awaited draft regulations for the non-testing deployment of autonomous vehicles.").

111. *See e.g.,* Johana Bhuiyan, *Michigan just became the first state to pass comprehensive self-driving regulations,* RECODE (Dec. 9, 2016), http://www.recode.net/2016/12/9/13890080/michigan-dot-self-driving-cars-laws-automakers.

112. S.B. 998, 98th Leg., Reg. Sess. (Mich. 2017), https://www.legislature.mi.gov/documents/2015-2016/publicact/pdf/2016-PA-0335.pdf.

113. S.B. 927 (Mich. 2016), http://www.legislature.mi.gov/documents/2015-2016/billengrossed/Senate/pdf/2016-SEBS-0927.pdf.

> shops that run diagnostics checks while fixing vehicles, owners who install new stereos, automated driving startups that modify production vehicles, researchers who test the safety of vehicle electronics, and many others. These bills are particularly troublesome in light of the assertion by some automakers that they alone "own" the software on vehicles that they have already sold. If these bills move forward, they should be limited to instances in which a person acts in willful or wanton disregard for the safety of others."

Legislators are not fully aware of all the nuances involved in "hacking", and the legitimate instances thereof (i.e. security research) which could lead to negative consequences for an essential part of ACV development and deployment.[114] In any case, such legislation could be a realistic alternative to copyright regulation of ACV jailbreaking.

IV. Conclusion

It is without doubt that ACVs will transform human mobility. It is also the case that ACV owners will be sufficiently incentivized to jailbreak their vehicles to unlock unauthorized functionality.

Liability could incur under the copyright regime, as well as the criminal and tort regimes, at both state and federal levels. Some or all jailbreak-side parties are vulnerable to such liability, depending on the nature of the event, from developers, distributors, installers, to end-users.

Given the current state of the law in this area, both technologists and policy makers should pay heed to the various scenarios envisioned in this paper and adjust their actions accordingly.

Technologists should seize upon the 2015 Exemptions to DMCA §1201, namely the vehicle modification and security research exemptions, and use that as a basis to justify the legal jailbreaking of ACVs for at least limited purposes – enabling owners to responsibly maximize the functionality of their product within the bounds of a safe and secure environment. Manufacturers should use as a model the relationship of other technology companies to their enthusiast jailbreaking communities, and try to build a similar symbiotic relationship.

Policy makers should realize that prohibiting ACV jailbreaking outright is anti-competitive, and that the incentives to jailbreak are too numerous and compelling to go unaddressed. ACV jailbreaking should be permitted under a narrow set of circumstances, and should not be regulated under the copyright system, but instead the main stakeholder in motor vehicle safety: NHTSA.

---

114. This is unusual, since the Michigan proposal is considered to be among the most advanced of state ACV development statutes (e.g., it does not require a certification process to be an ACV company, broadly defined).